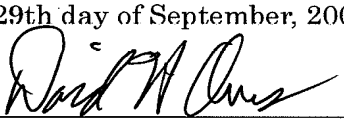
## CERTIFICATE OF VERIFICATION

I, David H. Owens

of Sumitomo Hamamatsucho Bldg. 3F, 1-18-16 Hamamatsucho, Minato-ku, Tokyo, Japan,

state that the attached document is a true and complete translation to the best of my knowledge of "Handbuch der Chipkarten".

Dated this 29th day of September, 2008.

Signature 

David H. Owens

**Handbook of Chip-cards**

Structure - Mode of operation - Use of Smart Cards

4. Revised and updated edition

Giesecke & Devrient GmbH

Patent and Licencing Dept.

Mr Bornhäuser

Postbox 80 07 29

81607 Munich

**Confirmation**

We hereby confirm that the book

***"Handbook of Chip-cards:*** *Structure – Mode of operation – Use of Smart Cards",*

authors: Wolfgang Rankl and Wolfgang Effling, with a preface by Jürgen Dethloff, 4th edition, published 2002, ISBN No. 3-446-22036-4, was despatched on 29.08.2002 and from then on was freely commercially available for ordering, i.e. it was accessible to the public.

The date of publication can be verified via the official German Library Database.

Carl Hanser Publishers GmbH & Co; KG.

(signed)

Dr. Hermann Riedel

Managing Editor

Technical Book Publishers

But the $I^2C$ bus, in widespread use in memories with serial access, is also used in chip-cards.

The functionality of the memory cards is most often optimized to a specific application. Due to this, the flexibility in the application is certainly very severely restricted, but on the other hand memory cards are particularly cheap. Typical applications for memory cards are prepaid telephone cards or health insurance cards.

Fig. 2.6: labels

| | |
|---|---|
| Anti-Kollisionsmechanismus | Anti-collision mechanism |
| Taktgenerator | Clock generator |
| Zugriffslogik | Access logic |
| Anwendungsdaten | Application data |
| Takt | Clock |
| Steuerleitung | Control line |
| Adress- und Sicherheitslogik | Address and security logic |
| Antenne | Antenna |
| Spannungsregelung | Voltage regulation |
| Reset-Erzeugung | Reset generation |
| Identifizierungsdaten | Identification data |
| Speicherchip | Storage chip |

Caption:

Typical architecture of a memory card with contactless interface and security logic. The diagram shows only the essential information and power flows and is not a circuit diagram.

### 2.3.2 Microprocessor cards

The heart of the chip of a microprocessor card is – as the name suggests – the processor, which is normally surrounded by four additional functional blocks: the mask ROM, the EEPROM, the RAM and the I/O port. Figure 2.7 shows the typical architecture of such a component.

Fig. 2.7 labels:

| | |
|---|---|
| Coprozessor | Coprocessor |
| Prozessor | Processor |
| Arbeitsspeicher | Working memory |
| Datenspeicher | Data memory |
| Betriebssytem[illegible] | Operating system [...] |
| Betriebssytem | Operating system |

Caption: Typical architecture of a contact-equipped microprocessor card, with coprocessor. The diagram shows only the essential information and power flows and is not a circuit diagram.

The mask ROM contains the operating system of the chip and is burned in during manufacture. As a condition of manufacturing, the content of the ROM is identical for all chips of a production batch and cannot be changed throughout the service life of the chip.

The EEPROM is the non-volatile storage area of the chip, in which data or else program code can be written and read under the control of the operating system.

The RAM is the working memory of the processor. This

storage area is volatile, and all data contained in it are lost when the supply voltage to the chip is switched off.

The serial I/O interface usually consists of only a single register, over which the data are transmitted in a bit-wise manner.

Microprocessor cards are very flexible in terms of their application. In the simplest case they contain a program optimized to a single application and are therefore also only usable for this one application.

Modern chip-card operating systems however enable different applications to be integrated in a single card. In this case the ROM contains only the basic commands of the operating system, while the application-specific parts of the program are not loaded into the EEPROM until after production of the card. Recent developments even enable applications to be retrospectively loaded into the chip-card, after the card has been personalized and issued to the card user. In this case, appropriate hardware and software measures are used to ensure that the different security conditions of such individual applications are not infringed. Specially optimized microprocessor chips for this application, with high computing power and memory capacity, have now become available.

### 2.3.3 Contactless chip-cards

Contacting to the contact-equipped chip-card takes place via the eight contacts specified in the ISO Standard 7816 Part 1. The reliability of the chip-cards with contacts has been constantly improved over the years, due to the increasing production experience of the manufacturers, so that for example the failure rates of telephone cards over a service life of one year are now significantly less than one per thousand. However, contacts remain one of the most frequent sources of faults in electromechanical systems. Defects can arise for example due to contamination by dirt, or wear on the contacts. In systems used in mobile devices, vibrations can lead to brief contact interruptions. Since the contacts on the surface of the chip-card are directly connected to the inputs of the integrated circuit, there is a danger that electrostatic discharges - several thousand Volts are certainly not uncommon - may weaken or even destroy the integrated circuit inside the card.

These technical problems are elegantly overcome by the contactless chip-card. Apart from these technical advantages though, the technology of contactless chip-cards also offers a range of interesting new application possibilities for the card issuer and the card user. For example, contactless chip-cards do not necessarily have to be inserted into a card reader, as there are systems which function over a distance of up to one meter.

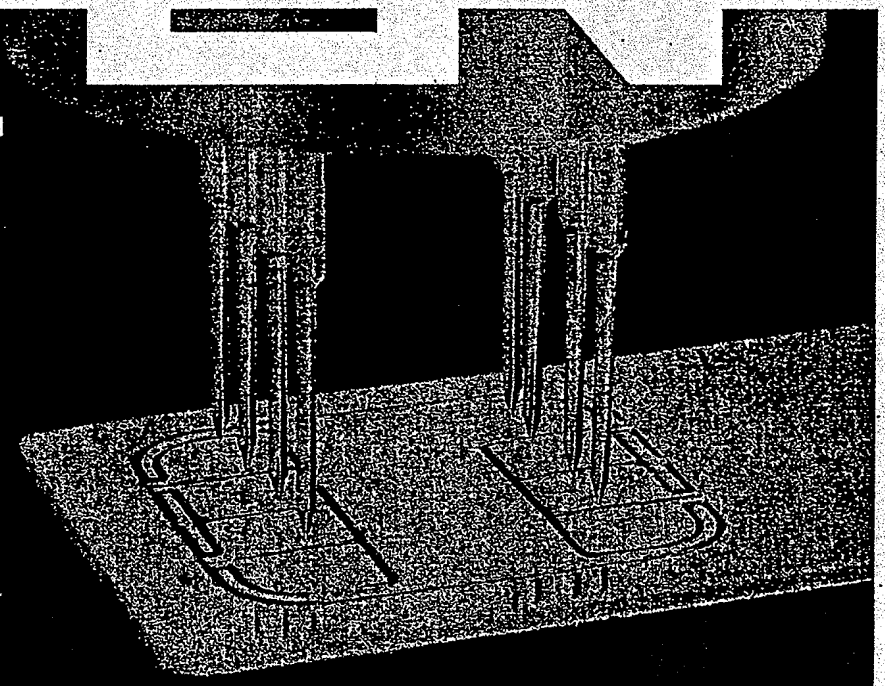
E1

Website zum Buch

Wolfgang Rankl
Wolfgang Effing

# Handbuch der Chipkarten

## Aufbau – Funktionsweise – Einsatz von Smart Cards



4., überarbeitete und aktualisierte Auflage

HANSER

HANSER

Giesecke & Devrient GmbH
Patent- und Lizenzabteilung
Herrn Bornhäuser
Postfach 80 07 29
81607 München

Dr. Hermann Riedel
Verlagsleiter Fachbuchverlag

Carl Hanser Verlag GmbH & Co. KG
Kolbergerstraße 22
D 81679 München
Telefon +49 (0)89 998 30 - 262
Telefax +49 (0)89 998 30 - 227
riedel@hanser.de
www.hanser.de

12. Januar 2007

**Bestätigung**

Hiermit bestätigen wir, dass da Buch

***Handbuch der Chipkarten: Aufbau - Funktionsweise - Einsatz***

Autoren: **Wolfgang Rankl und Wolfgang Effing** mit einem Vorwort von Jürgen Dethloff, 4. Auflage, Ausgabe 2002, ISBN-Nr. 3-446-22036-4, am 29.08.2002 ausgeliefert wurde und von da an im Handel frei bestellbar, d.h. der Öffentlichkeit zugänglich war.

Der Erscheinungstermin kann über die offizielle Datenbank derDeutschen Bibliothek nachgewiesen werden.

Carl Hanser Verlag GmbH & Co. KG

Dr. Hermann Riedel
Verlagsleiter
Fachbuchverlag

Carl Hanser Verlag GmbH & Co. KG
Postfach 86 04 20
D 81631 München
Telefon +49 (0)89 998 30 - 0
Telefax +49 (0)89 98 48 09
www.hanser.de

Geschäftsführung:
Wolfgang Beisler
Stephan Dr. Jaß
Michael Krüger

Sitz und Registergericht:
München HRA 43621
Ust-Id Nr.: DE 129 735 621

Persönlich haftende Gesellschafterin:
Carl Hanser Verwaltungsges. mbH
Sitz und Registergericht:
München HRB 40443

Deutsche Bank München
BLZ 700 700 10, Kto. 434 343 000
HypoVereinsbank München
BLZ 700 202 70, Kto. 863 700
Postbank München
BLZ 700 100 80, Kto. 77 15 - 809

ders einfache und damit preiswerte Realisierung im Chip ermöglicht. Es kommt aber auch der bei Speichern mit seriellem Zugriff weit verbreitete $I^2C$-Bus in Chipkarten zum Einsatz.

Die Funktionalität der Speicherkarten ist meist auf eine spezielle Anwendung hin optimiert. Hierdurch ist die Flexibilität in der Anwendung zwar stark eingeschränkt, dafür sind Speicherkarten aber auch besonders preisgünstig. Typische Anwendungen für Speicherkarten sind vorbezahlte Telefonkarten oder die Krankenversicherungskarte.

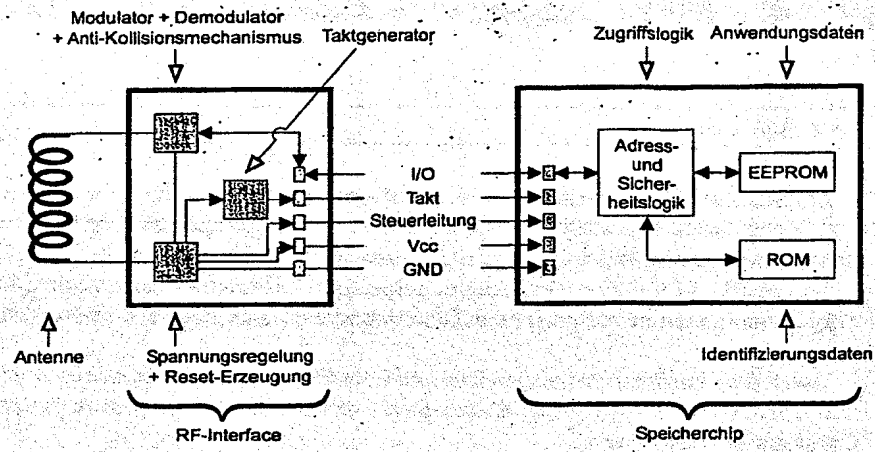



**Bild 2.6** Typische Architektur einer Speicherkarte mit kontaktlosem Interface und Sicherheitslogik. Die Abbildung zeigt lediglich die grundlegenden Informations- und Energieflüsse und ist kein Stromlaufplan.

## 2.3.2 Mikroprozessorkarten

Das Herz des Chips einer Mikroprozessorkarte ist – wie der Name schon sagt – der Prozessor, der in der Regel von vier weiteren Funktionsblöcken umgeben ist: dem Masken-ROM, dem EEPROM, dem RAM und dem I/O-Port. In Bild 2.7 ist die typische Architektur eines solchen Bausteins dargestellt.

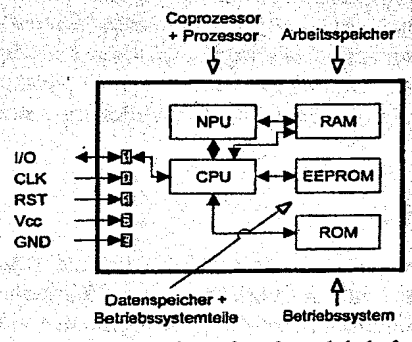



**Bild 2.7** Typische Architektur einer kontaktbehafteten Mikroprozessorkarte mit Koprozessor. Die Abbildung zeigt lediglich die grundlegenden Informations- und Energieflüsse und ist kein Stromlaufplan.

Das Masken-ROM enthält das Betriebssystem des Chips und wird während der Herstellung eingebrannt. Der Inhalt des ROM ist herstellungsbedingt für alle Chips eines Produktionsloses identisch und während der Lebensdauer des Chips unveränderbar.

Das EEPROM ist der nichtflüchtige Speicherbereich des Chips, in dem Daten oder auch Programmcode unter Kontrolle des Betriebssystems geschrieben und gelesen werden können.

Das RAM ist der Arbeitsspeicher des Prozessors. Dieser Speicherbereich ist flüchtig, und alle darin gespeicherten Daten gehen verloren, wenn die Versorgungsspannung des Chips abgeschaltet wird.

Die serielle I/O-Schnittstelle besteht meist nur aus einem einzigen Register, über welches die Daten Bit für Bit übertragen werden.

Mikroprozessorkarten sind in der Anwendung sehr flexibel. Im einfachsten Fall enthalten sie ein auf eine einzige Anwendung hin optimiertes Programm und sind somit auch nur für diese eine Anwendung verwendbar.

Moderne Chipkartenbetriebssysteme ermöglichen jedoch, verschiedene Anwendungen in einer einzigen Karte zu integrieren. Das ROM enthält in diesem Falle nur die Basiskommandos des Betriebssystems, während die anwendungsspezifischen Teile des Programms erst nach der Kartenproduktion in das EEPROM geladen werden. Neue Entwicklungen ermöglichen es sogar, Anwendungen in die Chipkarte nachzuladen, nachdem die Karte personalisiert und an den Kartenbenutzer ausgegeben wurde. Durch entsprechende Hardware- und Softwaremaßnahmen wird hierbei sichergestellt, dass die unterschiedlichen Sicherheitsbedingungen der einzelnen Anwendungen hierbei nicht verletzt werden. Speziell hierfür optimierte Mikroprozessorchips mit hoher Rechenleistung und Speicherkapazität sind mittlerweile verfügbar.

### 2.3.3 Kontaktlose Chipkarten

Die Kontaktierung der kontaktbehafteten Chipkarte erfolgt über die acht in der ISO-Norm 7816 Teil 1 festgelegten Kontakte. Die Zuverlässigkeit der Chipkarten mit Kontakten konnte aufgrund der steigenden Produktionserfahrung der Hersteller in den vergangenen Jahren stetig verbessert werden, sodass zum Beispiel die Ausfallquote von Telefonkarten über eine Lebensdauer von einem Jahr heute deutlich unter ein Promille liegt. Nach wie vor sind jedoch Kontakte eine der häufigsten Fehlerquellen in elektromechanischen Systemen. Störungen können zum Beispiel durch Verschmutzung oder Abnutzung der Kontakte entstehen. Beim Einsatz in mobilen Geräten können Vibrationen zu kurzzeitigen Kontaktunterbrechungen führen. Da die Kontakte auf der Oberfläche der Chipkarte direkt mit den Eingängen der integrierten Schaltung verbunden sind, besteht die Gefahr, dass elektrostatische Entladungen – einige tausend Volt sind durchaus keine Seltenheit – die integrierte Schaltung im Innern der Karte schwächen oder gar zerstören.

Diese technischen Probleme werden von der kontaktlosen Chipkarte elegant umgangen.

Außer diesen technischen Vorteilen bietet die Technik der kontaktlosen Chipkarte aber auch eine Reihe interessanter neuer Möglichkeiten in der Anwendung für den Kartenherausgeber und den Kartenbenutzer. So müssen kontaktlose Chipkarten zum Beispiel nicht unbedingt in einen Kartenleser eingesteckt werden, sondern es gibt Systeme, die über eine Entfernung von bis zu einem Meter funktionieren. Dies ist beispielsweise in Zugangskon-